

CLAIMS

We claim:

1. A method for improving the handling of personally identifiable information, said method comprising:
5 identifying the parties involved in a process of handling personally identifiable information;
identifying the data involved in said process;
classifying the data;
expressing each relationship between each pair of said parties
10 in terms of a privacy agreement; and
representing said parties, said data, and said privacy agreements graphically in one or more privacy agreement relationship diagrams,
wherein:
15 said privacy agreement uses a limited number of privacy-related actions concerning said personally identifiable information;
said privacy agreement expresses rules regarding said privacy-related actions, for each of said parties; and
said privacy agreement is specific to a single purpose.
20
2. The method of Claim 1, further comprising mapping a business process to the privacy rules that should govern the behavior of each pair of parties.
- 25 3. The method of Claim 1, further comprising identifying opportunities to reduce privacy-related risks involved in said process.
4. The method of Claim 3, further comprising identifying
30 unnecessary exchanges of data, for possible elimination.

5. The method of Claim 3, further comprising identifying opportunities to transform data into a less sensitive form.

6. A system for improving the handling of personally identifiable information, said system comprising:
5 means for identifying the parties involved in a process of handling personally identifiable information;
means for identifying the data involved in said process;
means for classifying the data;
10 means for expressing each relationship between each pair of said parties in terms of a privacy agreement; and
means for representing said parties, said data, and said privacy agreements graphically in one or more privacy agreement relationship diagrams,
15 wherein;
said privacy agreement uses a limited number of privacy-related actions concerning said personally identifiable information;
said privacy agreement expresses rules regarding said privacy-related actions, for each of said parties; and
20 said privacy agreement is specific to a single purpose.

7. The system of Claim 6, further comprising means for mapping a business process to the privacy rules that should govern the behavior of each pair of parties.

8. The system of Claim 6, further comprising means for identifying opportunities to reduce privacy-related risks involved in said process.

9. The system of Claim 8, further comprising means for

identifying unnecessary exchanges of data, for possible elimination.

10. The system of Claim 8, further comprising means for identifying opportunities to transform data into a less sensitive form.

11. A computer-usable medium having computer-executable instructions for improving the handling of personally identifiable information, said computer-executable instructions comprising:

means for identifying the parties involved in a process of handling personally identifiable information;

means for identifying the data involved in said process;

means for classifying the data;

means for expressing each relationship between each pair of said parties in terms of a privacy agreement; and

means for representing said parties, said data, and said privacy agreements graphically in one or more privacy agreement relationship diagrams,

wherein;

said privacy agreement uses a limited number of privacy-related actions concerning said personally identifiable information;

said privacy agreement expresses rules regarding said privacy-related actions, for each of said parties; and

said privacy agreement is specific to a single purpose.

12. The computer-usable medium of Claim 11, further comprising means for mapping a business process to the privacy rules that should govern the behavior of each pair of parties.

13. The computer-usable medium of Claim 11, further comprising means for identifying opportunities to reduce privacy-related risks involved in said process.

5 14. The computer-usable medium of Claim 13, further comprising means for identifying unnecessary exchanges of data, for possible elimination.

10 15. The computer-usable medium of Claim 13, further comprising means for identifying opportunities to transform data into a less sensitive form.